UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT CHATTANOOGA

DEWEY MASON, *individually and on behalf of all others similarly situated*,	)	
	)	No. 1:24-cv-384
Plaintiff,	)	
v.	)	Judge Curtis L. Collier
	)	Magistrate Judge Christopher H. Steger
WRIGHT BROTHERS CONSTRUCTION COMPANY, INC.,	)	
Defendant.	)	

M E M O R A N D U M

Before the Court is a motion by Defendant, Wright Brothers Construction Company, Inc., to dismiss the class-action complaint pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure for failure to state a claim on which relief can be granted. (Doc. 10.) Plaintiff, Dewey Mason, has responded (Doc. 17), and Defendant has replied (Doc. 20). This matter is now ripe for review.

I. BACKGROUND[1]

Defendant Wright Brothers Construction Company, Inc. is a construction company with its principal place of business and place of incorporation in Tennessee. (Doc. 1-1 ¶ 9.) Plaintiff Dewey Mason is a former employee of Defendant who resides in Georgia. (*Id.* ¶¶ 8, 68.) This class action stems from an alleged data breach. (*Id.* ¶¶ 1–2.)

Cyberattacks and data breaches have become more common. (*Id.* ¶¶ 20–21.) Cyberattacks often involve the acquisition of individuals' personally identifiable information ("PII"), which "remains of high value to criminals." (*Id.* ¶ 36.) The Federal Trade Commission ("FTC") defines

[1] This summary of the facts accepts all the factual allegations in Plaintiff's complaint as true. *See Gunasekera v. Irwin*, 551 F.3d 461, 466 (6th Cir. 2009).

identifying information as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." 17 C.F.R. § 248.201. "Based on the value of the information stolen, the data either has or will be sold to cybercriminals" who then "misuse it and earn money from financial fraud and identity theft of data breach victims." (Doc. 1-1 ¶ 65.) PII is highly sought after, especially when "it includes Social Security numbers and other government identification, which is significantly difficult if not impossible to change." (*Id*. ¶ 38.)

According to Plaintiff's class-action complaint, Plaintiff was required to provide his PII to Defendant as a condition of his employment. (*Id*. ¶ 68.) In April 2024, Defendant experienced what it thought to be "technical issues." (*Id*. ¶ 2.) It subsequently learned, however, that hackers gained access to its information systems between April 3 and April 5, 2024. (*Id*.) The hackers "took certain files" containing the PII of Plaintiff and the proposed class members, including their Social Security numbers. (*Id*.)

The data breach was allegedly caused by Akira, "a notorious cybergang known for taking advantage of a company's failure to properly update its information systems and devices with the appropriate security patches and for failing to implement basic cybersecurity measures like multi-factor authentication." (*Id*. ¶ 5.) Plaintiff alleges Akira exfiltrated at least twelve gigabytes of data, including "financial records, accounting documents, insurance information, and employee files." (*Id*. ¶ 6.)

Plaintiff asserts that as a custodian of PII, "Defendant knew, or should have known," the importance of safeguarding PII (*id*. ¶¶ 22, 24, 32), and suggests the results of the data breach were "directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures" (*id*. ¶¶ 25, 34). More specifically, Plaintiff asserts Defendant failed to properly implement basic data security practices; failed to audit, monitor, or ensure the integrity of its data

security practices; and failed to appropriately prepare for a potential data breach and respond to it in a timely manner. (*Id.* ¶ 45.) Plaintiff also alleges Defendant failed to comply with the industry standards set forth and published by the FTC (*id.* ¶ 46), as well as frameworks established in "reasonable cybersecurity readiness" (*id.* ¶ 51).

As a result of the breach, Plaintiff alleges that he and the proposed class members have all sustained actual injuries and damages including: (1) invasion of privacy; (2) loss of time and productivity incurred in mitigating the identity-theft risk; (3) the loss of value in their PII without the benefit of the bargain; and (4) the continued risk to their PII, which is subject to further breaches. (*Id.* ¶ 53.)

Plaintiff claims that exposure of his sensitive PII represents a serious invasion of his privacy and he now has an increased risk of identity theft and fraud "for years to come." (*Id.* ¶¶ 76–77.) Consequently, Plaintiff has sustained emotional distress and experienced stress and anxiety. (*Id.* ¶¶ 72–73.) Further, after the breach, Plaintiff has experienced a significant increase of phishing attempts made against him daily, with the number of attempts sometimes reaching dozens per day. (*Id.* ¶ 74.) He has also received numerous phone calls from "fraudsters" trying to convince him to pay them money. (*Id.*) Plaintiff also alleges he has "suffered lost time, interference, and inconvenience" trying to mitigate the data breach. (*Id.* ¶ 73.) He asserts he has had to monitor accounts and credit scores which "took away from other activities and work duties." (*Id.* ¶ 72.)

According to Plaintiff, "[t]he ramifications of Defendant's failure to keep secure the PII . . . are long lasting and severe" because "[o]nce PII is stolen, fraudulent use of that information and damage to victims may continue for years." (*Id.* ¶ 26.) Harm resulting from the data breach "may not come to light for years" and "[t]here may be a time lag between when harm occurs versus when

it is discovered, and also between when PII is stolen and when it is used." (*Id.* ¶ 40.) As a result, Plaintiff must "spend considerable time and money on an ongoing basis to try to mitigate and address these impending harms." (*Id.* ¶ 76.) Specifically, Plaintiff and the proposed class members must pay for credit and identity-theft monitoring for a minimum of seven years, which can cost two hundred dollars or more per year. (*Id.* ¶ 67.)

Furthermore, Plaintiff alleges he suffered a loss of value in his PII. (*Id.* ¶ 31.) There is an "active and robust legitimate marketplace for PII." (*Id.* ¶ 28.) Consumers can sell non-public information to a data broker who "aggregates the information and provides it to markets or app[lication] developers." (*Id.* ¶ 29.) One company pays fifty dollars per year to people who agree to provide the company with their web browsing history. (*Id.* ¶ 30.) Plaintiff contends that his PII "has been damaged and diminished by its compromise and unauthorized release." (*Id.* ¶ 31.) Thus, as a result of Plaintiff's PII being released without compensation and "the rarity of the data" being lost, Plaintiff alleges he suffered economic loss. (*Id.*)

Based on these allegations, Plaintiff filed a class-action complaint against Defendant in the Chancery Court of Bradley County, Tennessee, on October 31, 2024. (Doc. 1-1.) Plaintiff brought this suit on behalf of himself and all members of the proposed class defined as: "[a]ll individuals residing in the United States whose PII was compromised in the [d]ata [b]reach and to whom Defendant sent an individual notification that they were affected by the [d]ata [b]reach." (*Id.* ¶ 78; Doc. 1 at 7.) Plaintiff asserts claims for (1) negligence; (2) negligence per se; (3) breach of implied contract; and (4) breach of bailment. (Doc. 1-1 ¶¶ 90–122.) On December 11, 2024, Defendant removed the action to this Court (Doc. 1), and on December 18, 2024, Defendant moved to dismiss the class-action complaint (Doc. 10). This matter is now ripe for review.

II. STANDARD OF REVIEW

A defendant may move to dismiss a claim for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). In ruling on a motion to dismiss under Rule 12(b)(6), a court must accept all the factual allegations in the complaint as true and construe the complaint in the light most favorable to the plaintiff. *Gunasekera v. Irwin,* 551 F.3d 461, 466 (6th Cir. 2009) (quoting *Hill v. Blue Cross & Blue Shield of Mich.*, 49 F.3d 710, 716 (6th Cir. 2005)). A court is not, however, bound to accept bare assertions of legal conclusions as true. *Papasan v. Allain*, 478 U.S. 265, 286 (1986); *see 16630 Southfield Ltd. P'ship v. Flagstar Bank, F.S.B.*, 727 F.3d 502, 506 (6th Cir. 2013). "'[N]aked assertions devoid of further factual enhancement' contribute nothing to the sufficiency of the complaint." *Flagstar Bank*, 727 F.3d at 506 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

In deciding a motion under Rule 12(b)(6), a court must determine whether the complaint contains "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Although a complaint need only contain a "short and plain statement of the claim showing that the pleader is entitled to relief," *Iqbal*, 556 U.S. at 677–78 (quoting Fed. R. Civ. P. 8(a)(2)), this statement must nevertheless contain "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 678. Plausibility "is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (quoting *Twombly*, 550 U.S. at 556). "[W]here the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not 'show[n]'—'that the pleader is entitled to relief.'" *Id.* at 679 (alteration in original) (quoting Fed. R. Civ. P. 8(a)(2)).

"Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678.

III. DISCUSSION

The Court will first address the parties' choice-of-law arguments, followed by the effect of Tennessee Code Annotated § 29-34-215 on Plaintiff's claims. The Court will then address Plaintiff's claims for negligence, negligence per se, breach of implied contract, and breach of bailment in turn.

A. Choice of Law

As a preliminary matter, the Court must address its jurisdiction to handle this case. A class action in federal court is governed by 28 U.S.C. § 1332(d), as amended by the Class Action Fairness Act of 2005, Pub. L. No. 109-2, 119 Stat. 4 (2005) ("CAFA"). CAFA confers federal jurisdiction over certain class actions where: (1) the proposed class contains at least one hundred members; (2) minimal diversity exists between the parties; and (3) the aggregate amount in controversy exceeds $5,000,000. 28 U.S.C. § 1332(d).

Here, this Court has jurisdiction because the class-action complaint meets the CAFA requirements. First, the proposed class action contains at least one hundred members, as the complaint alleges that the data breach "likely affected thousands of [Defendant's] current and former employees." (Doc. 1-1 ¶ 7.) Second, Defendant is a citizen of Tennessee and Plaintiff is a citizen of Georgia (*id*. ¶¶ 8–9), meaning at least one member of the class is a citizen of a different state than Defendant. Finally, while the complaint does not allege a specific amount in controversy, there is a plausible allegation the amount in controversy exceeds five million dollars given the large class size and request for compensatory damages and attorneys fees. *See Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 89 (2014) (explaining a defendant

can establish the amount in controversy by an unchallenged, plausible assertion in its notice of removal).

Because the Court has jurisdiction, the Court must now determine which state's law applies to Plaintiff's claims. "A federal court sitting in diversity ordinarily must follow the choice-of-law rules of the State in which it sits." *Atlantic Marine Const. Co v. U.S. Dist. Ct. for the W. Dist. of Tex.*, 571 U.S. 49, 65 (2013) (citation omitted). In tort cases, Tennessee law applies the "most significant relationship test," which provides that the law of the state where the injury occurred applies unless some other state has a more significant relationship to the litigation. *Hataway v. McKinley*, 830 S.W.2d 53, 59 (Tenn. 1992). To determine the state with the most significant relationship, courts must consider several factors: (1) the place where the injury occurred; (2) the place where the conduct causing the injury occurred; (3) the domicile, residence, nationality, place of incorporation, and place of business of the parties; and (4) the place where the relationship, if any, between the parties is centered. *Id.* In contract cases, Tennessee law provides that a contract is governed by the law of the state where it was executed. *See Williams v. Smith*, 465 S.W.3d 150, 153 (Tenn. Ct. App. 2014) (citation omitted).

Defendant argues Plaintiff's alleged injuries such as receiving numerous phone calls and phishing attempts most likely occurred in Georgia, where Plaintiff is domiciled. (Doc. 11 at 10 (citing Doc. 1-1 ¶¶ 8, 72–74).) It argues Georgia law should apply since "the injury occurred there and no state has a more significant relationship." (*Id.*)

The Court disagrees. Defendant operates in multiple states and the proposed class is nationwide. (Doc. 1-1 ¶ 7.) This means the domiciles of Plaintiff and the proposed class members most likely vary. While some of the alleged injuries might have taken place in Georgia where Plaintiff is domiciled, some of the alleged injuries also likely occurred in different states. *See*

Haney v. Charter Foods N., LLC, No. 2:23-cv-46, 2024 WL 4054361, at *6 (E.D. Tenn. Aug. 28, 2024) (noting that a nation-wide class is significant when considering the location of alleged injuries).

Thus, the Court must look to the other factors to determine which state has the most significant relationship. The parties agree the data breach appears to have occurred in Tennessee. (Doc. 11 at 10; Doc. 17 at 6.) Defendant, "whose conduct is the common denominator among the proposed class," has its principal place of business in Tennessee and its existence is governed by Tennessee law. *Haney*, 2024 WL 4054361, at *6. For these reasons, the Court finds Tennessee is the state with the most significant relationship and will apply Tennessee law to the tort claims. *See In re Numotion Data Incident Litig.*, No. 3:24-CV-00545, 2025 WL 57712, at *7 (M.D. Tenn. Jan. 9, 2025) ("While the proposed class is nationwide, meaning that the named plaintiffs' and the putative class members' domiciles vary and that the alleged injuries occurred in different states, the data breach occurred in Tennessee, and the defendant is based in Tennessee.") The Court will also apply Tennessee law to the implied-contract claim for the same reasons; "although there is not a written contract, any contractual duties were bestowed on [a] Tennessee-based business[], and the alleged breach-of-implied-contract claim relies on actions taken in Tennessee." *Haney*, 2024 WL 4054361, at *6.

B. Effect of Amended Tennessee Law on Plaintiff's Claims

Defendant argues that Tennessee Code Annotated § 29-34-215, enacted on May 21, 2024, bars Plaintiff's class claims. (Doc. 11 at 7–9.) Section 29-34-215 provides in relevant part, "[a] private entity is not liable in a class action lawsuit resulting from a cybersecurity event unless the cybersecurity event was caused by willful and wanton misconduct or gross negligence on the part of the private entity." Tenn. Code Ann. § 29-34-215(1)(b). While Section 2 states that "[t]his act

takes effect upon becoming a law," the statute does not expressly state that it applies retroactively. *See* Tenn. Code Ann. § 29-34-215. Defendant contends, however, that § 29-34-215 does apply retroactively and that the class action should be barred because "Plaintiff has not alleged, nor attempted to allege, that [Defendant] acted with willful and wanton misconduct or gross negligence with regards to safeguarding Plaintiff's PII." (*Id*. at 9.)

"Generally, statutes are presumed to operate prospectively and not retroactively." *Kee v. Shelter Ins.*, 852 S.W.2d 226, 228 (Tenn. 1993) (citing *Woods v. TRW, Inc.*, 557 S.W.2d 274, 275 (Tenn. 1977) & *Cates v. T.I.M.E., DC, Inc.*, 513 S.W.2d 508, 510 (Tenn. 1974)). To overcome this presumption, a statute must be "remedial or procedural in nature." *Kee*, 852 S.W.2d at 228. "A procedural or remedial statute is one that does not affect the vested rights or liabilities of the parties. A procedural statute is one that addresses the mode or proceeding by which a legal right is enforced." *In re D.A.H.*, 142 S.W.3d 267, 273 (Tenn. 2004) (quoting *Nutt v. Champion Int'l Corp.*, 980 S.W.2d 365, 368 (Tenn. 1998)).

Only two court decisions have addressed § 29-34-215—*Haney v. Charter Foods North, LLC*, No. 2:23-cv-46, 2024 WL 4054361 (E.D. Tenn. Aug. 28, 2024) and *Cahill v. Memorial Heart Institute, LLC*, No. 1:23-cv-168, 2024 WL 4311648 (E.D. Tenn. Sept. 26, 2024). In both cases, the court held that § 29-34-215 does not apply retroactively.

In *Haney*, the court found § 29-34-215 "is focused predominantly on substantive law related to cybersecurity." 2024 WL 4054361, at *23 (citing Tenn. Code Ann. § 29-34-215) (emphasis removed) (noting that the statute's reference to class actions represents the extent of its procedural or remedial interests). The court explained that rather than barring class actions categorically, § 29-34-215 "draws its distinction based on a defendant's *substantive* conduct"—i.e., whether a defendant acted with willful and wanton misconduct or gross negligence. *Id*.

(emphasis in original). Accordingly, the statute "goes beyond merely affecting the procedural privilege to proceed as a class action," and instead "alters the 'vested rights and liabilities of the parties' by heightening the mens rea required for defendants to be liable." *Id*. at *23–24 (quoting *In re D.A.H.*, 142 S.W.3d at 273). The court held that "[g]iven the generally substantive nature of the . . . statute and its heightened mens rea requirement—and in light of the presumption of prospective application," the statute does not apply retroactively. *Id*. at *24. In *Cahill*, this Court agreed with the analysis in *Haney* and found that § 29-34-215 did not retroactively apply to the pending litigation. 2024 WL 4311648, at *5.

Despite these holdings, Defendant argues that this case differs from *Haney* and *Cahill* because those cases "focused on whether the statute can be retroactively applied to pending litigation, not [a lawsuit] filed after the statute." (Doc. 11 at 8.) Defendant admits that the data breach in this case allegedly occurred in April 2024, just a month before § 29-34-215's effective date. (*Id*.) However, Defendant suggests that because Plaintiff filed his complaint in October 2024, more than five months after the passing of the statute, the statute should apply retroactively because Plaintiff had "ample notice of [§ 29-34-215's] heightened pleading standard." (*Id*.) Further, Defendant seems to suggest that this case is different because the conduct happened just a month before the statute's effective date rather than nine months before the statute's effective date. (*Id*.)

In response, Plaintiff argues that *Haney* and *Cahill* are similar to this case and that § 29-34-215 should not be applied retroactively because the alleged conduct still happened a month before the statute went into effect. (Doc. 17 at 3–4.) He states, "Defendant asks the Court to abandon the bright-line rule and accept a malleable standard in which a statute can somehow be a little retroactive but not a lot. Defendant cites no authority for this bizarre proposition." (*Id*.)

The Court agrees with Plaintiff. Even though Plaintiff filed his complaint more than five months after the passing of the statute, § 29-34-215's heightened pleading standard does not apply here because the alleged conduct occurred in April 2024, one month before the statute went into effect. The fact that the alleged conduct happened only one month before the statute's effective date is immaterial. The alleged conduct still predated the date on which the statute became operative and enforceable, whether it happened a year, month, or day prior to the statute's effective date. Like in *Haney* and *Cahill*, the Court finds that § 29-34-215 does not apply retroactively and cannot bar Plaintiff's claims on this basis. Accordingly, the Court need not reach the issue of whether the complaint sufficiently alleges a mens rea that would satisfy § 29-34-215.

C. Defendant's Motion to Dismiss Plaintiff's Claims

The Court will next address each of Plaintiff's claims to determine whether they state a claim for which relief can be granted.

1. Negligence

The class-action complaint first alleges a claim for negligence. (Doc. 1-1 ¶¶ 90–109.) Under Tennessee law, to make a prima facie claim of negligence, a plaintiff must establish five elements: (1) a duty of care owed by the defendant to the plaintiff; (2) conduct by the defendant falling below the standard of care amounting to a breach of that duty; (3) damages; (4) causation in fact; and (5) proximate or legal cause. *Giggers v. Memphis Hous. Auth.*, 277 S.W.3d 359, 364 (Tenn. 2009). "No claim for negligence can succeed in the absence of any one of these elements." *Cox v. M.A. Primary & Urgent Care Clinic*, 313 S.W.3d 240, 259 (Tenn. 2010) (citation omitted).

Defendant does not contest that Plaintiff sufficiently pleaded the elements of duty, breach, or causation, but does contest that Plaintiff sufficiently pleaded the element of damages. (*See* Doc.

11 at 12; Doc. 20 at 5.) Defendant argues "that there are insufficient allegations of damages stemming from the data breach." (Doc. 20 at 5 (quoting *Western Sizzlin, Inc. v. Harris*, 741 S.W.2d 334, 336 (Tenn. Ct. App. 1987) ("[U]ncertain, contingent, or speculative damages should not be awarded.")).) Therefore, the Court will only address the element of damages.

"An award of damages, which is intended to make a plaintiff whole, compensates the plaintiff for damage or injury caused by a defendant's wrongful conduct." *Dedmon v. Steelman*, 535 S.W.3d 431, 437 (Tenn. 2017) (quoting *Meals ex rel. Meals v. Ford Motor Co.*, 417 S.W.3d 414, 419 (Tenn. 2013)). "The party seeking damages has the burden of proving them." *Id.* (quoting *Overstreet v. Shoney's, Inc.*, 4 S.W.3d 694, 703 (Tenn. Ct. App. 1999)). A prevailing plaintiff may recover economic and non-economic damages. *Dedmon*, 535 S.W.3d at 437 (citing *Meals*, 417 S.W.3d at 419–20).

Economic damages are quantifiable expenses that naturally result from the defendant's wrongful conduct. *Meals*, 417 S.W.3d at 419. These damages "have a monetary value that is readily ascertainable," such as medical expenses, future medical expenses, lost wages, and lost earning potential. *Health Cost Controls, Inc. v. Gifford*, 239 S.W.3d 728, 733 (Tenn. 2007). Non-economic damages result from "pain and suffering, permanent impairment and/or disfigurement, and loss of enjoyment of life." *Meals*, 417 S.W.3d at 420 (internal citations omitted). These damages are generally "highly subjective and are not susceptible to proof by a specific dollar amount." *Dedmon*, 535 S.W.3d at 438.

Here, Defendant argues that Plaintiff's allegations are insufficient to support the element of damages because Plaintiff "cites only to vague references of spam phone calls, lost time, emotional distress and a possible future injury." (Doc 11 at 12.) Defendant further contends that "Plaintiff's allegations regarding time spent dealing with the data incident are not quantified in

any way, nor does Plaintiff plead specifics as to whether he spent any money dealing with the data incident." (*Id*.)

In response, Plaintiff argues he has pleaded sufficient damages. First, Plaintiff argues he and the proposed class members "face years of substantial increases in identity theft and fraud" that they will have to continue to carefully monitor, especially because Social Security numbers were acquired. (Doc. 17 at 7 (citing Doc. 1-1 ¶ 122).) Second, Plaintiff argues he has suffered a severe invasion of privacy—"a harm long recognized in American courts." (*Id.* at 8 (citing Doc. 1-1 ¶¶ 70, 77).) Next, Plaintiff alleges damages for time lost in dealing with daily scam and phishing attempts. (*Id*. (citing Doc. 1-1 ¶ 74).) Finally, Plaintiff alleges diminished value of his private information in which "Defendant failed to provide the benefit of the bargain." (*Id.* (citing Doc. 1-1 ¶¶ 115, 117).)

Defendant's arguments regarding Plaintiff's alleged damages for time lost and diminished value of his PII are well taken. *See In re Numotion.*, 2025 WL 57712, at *14–15 (finding Tennessee courts have not awarded damages for lost time spent mitigating a data breach and holding there is no injury for diminished value of PII where the plaintiffs have not alleged they can no longer sell their information). Nevertheless, "credit monitoring may be compensable where evidence shows that the need for future monitoring is a reasonably certain consequence of the defendant's breach of duty." *Id.* at *13 (quoting *Greenstein v. Noblr Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1229 (N.D. Cal. 2022)). "[T]he hacking of highly sensitive information, particularly including Social Security numbers . . . is usually considered to give rise to a sufficiently real and imminent risk of identity theft to warrant monitoring." *Id.* (citation omitted).

At this stage, the Court draws all reasonable inferences in favor of Plaintiff. Plaintiff alleges that due to Defendant's failure to safeguard its information systems, hackers "took certain

files" containing the PII of Plaintiff and the proposed class members, including their Social Security numbers. (Doc. 1-1 ¶ 2.) Due to the hacking of this highly sensitive information, Plaintiff alleges that he and the proposed class members must pay for future credit and identity-theft monitoring for a minimum of seven years, which could cost two hundred dollars or more per year. (*Id.* ¶ 67.) Consequently, Plaintiff alleges he has sustained emotional distress and experienced stress and anxiety. (*Id*. ¶¶ 72–73.)

Given the type of data stolen here, privacy harm and an increased risk of identity theft are cognizable injuries. *See Allen v. Wenco Mgmt., LLC,* 696 F. Supp. 3d 432, 437–38 (N.D. Ohio 2023). The Court finds that Plaintiff has alleged facts that, if true, would entitle him to recover the reasonable and necessary cost of future credit monitoring. *See In re Numotion*, 2025 WL 57712, at *16. Along with these monetary damages, Plaintiff may also be "entitled to recover emotional injury" for "the anxiety associated with the fear of identity theft" he alleges. *Id.* Therefore, viewing the facts in the light most favorable to Plaintiff, Plaintiff has alleged cognizable damages arising from Defendant's negligence in securing the PII. Accordingly, Defendant's motion to dismiss Plaintiff's negligence claim will be **DENIED.**

2. Negligence Per Se

The class action complaint also alleges a claim of negligence per se. (Doc. 1-1 ¶¶ 90–109.) To make a prima facie case of negligence per se, a plaintiff must establish three elements: (1) a violation of a statutory or regulatory duty of care; (2) a showing that the statute or regulation was meant to benefit and protect the injured party; and (3) proximate cause. *Steinberg v. Luedtke Trucking, Inc.*, No. 4:17-cv-9, 2018 WL 3233341, at *3 (E.D. Tenn. July 2, 2018) (citing *Chase,*

Jr. v. Physiotherapy Assocs., Inc., No. 02A01-9607-CV-00171, 1997 WL 572935, at *5 (Tenn. Ct. App. Sept. 5, 1997)).

"The negligence per se doctrine does not create a new cause of action." *Rains v. Bend of the River*, 124 S.W.3d 580, 589 (Tenn. Ct. App. 2003) (citations omitted). Instead, "it is a form of ordinary negligence that enables the courts to use a penal statute to define a reasonably prudent person's standard of care." *Id.* (citations omitted). But "[n]ot every statutory violation amounts to negligence per se." *Id*. at 590 (citation omitted). "To trigger the doctrine, the statute must establish a specific standard of conduct." *Id*. (citations omitted). Among other factors, courts must consider "whether the statute clearly defines the prohibited or required conduct." *Id.* at 591.

Plaintiff claims Defendant violated the statutory standards of care under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. (Doc. 1-1 ¶¶ 94, 101.) Defendant moves to dismiss Plaintiff's negligence per se claim on the grounds that the FTC Act does not establish a specific standard of conduct. (Doc. 20 at 6.) It argues, "Plaintiff's reliance on extra[-] statutory sources implicitly concedes that the FTC Act does not provide a standard of care and his negligence *per se* claim therefore fails under Tennessee law." (*Id*. at 7.)

Section 5 of the FTC Act provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a)(1). In the complaint, Plaintiff references materials and guides promulgated by the FTC "which highlight the importance of implementing reasonable data security practices" to businesses. (Doc. 1-1 ¶ 41.) Rather than citing the FTC Act itself to define the standard of care required of Defendant, Plaintiff cites to these resources. (*See id.* ¶¶ 41–44.)

Plaintiff's reliance on extra-statutory FTC guidance indicates a concession that the statute does not define a standard of care. *See In re HCA Healthcare, Inc. Data Sec. Litig.*, 2024 WL

3857330, at *4 (M.D. Tenn. Aug. 15, 2024) (holding the plaintiffs' reliance on "extra-statutory sources to determine what constitutes an 'unfair' cybersecurity practice . . . implicitly concede[d] that the statute itself provides no such answer" (quoting *Allen*, 696 F. Supp. at 440) (noting the FTC Act does not set forth a definite standard of care required to support a negligence per se claim)). Therefore, because the FTC Act does not establish a specific standard of conduct, Plaintiff's negligence per se claim fails. *See Rains*, 124 S.W.3d at 591. Accordingly, Defendant's motion to dismiss Plaintiff's negligence per se claim will be **GRANTED**. Plaintiff's negligence per se claim will be **DISMISSED WITH PREJUDICE**.

3. Breach of Implied Contract

Next, the class-action complaint alleges a claim for breach of implied contract. (Doc. 1-1 ¶¶ 110–17.) In Tennessee, the elements of breach of a contract implied in fact ("implied contract") are (1) existence of an enforceable contract, (2) nonperformance amounting to a breach of the contract, and (3) damages caused by the breach of contract. *Bancorp South Bank, Inc. v. Hatchel*, 223 S.W.3d 223, 227 (Tenn. Ct. App. 2006). "[I]n order for a contract implied in fact to be enforceable, it must be supported by mutual assent, consideration, and lawful purpose." *Thompson v. Hensley*, 136 S.W.3d 925, 930 (Tenn. Ct. App. 2003). A contract "must result from a meeting of the minds of the parties in mutual assent to the terms." *Johnson v. Cent. Nat'l Ins. Co. of Omaha, Neb.*, 356 S.W.2d 277, 281 (Tenn. 1962) (citation omitted).

Defendant argues that "Plaintiff has not identified any term, provision, contractual language, or other action of [Defendant] to support his breach of implied contract claim. (Doc. 11 at 13.) Defendant also argues, "Plaintiff does not allege any facts that establish a meeting of the minds between [Defendant] and Plaintiff as to data protection or data security services." (*Id*. at 14.) In response, Plaintiff argues that by him providing his PII, and Defendant's acceptance of the

information, the parties mutually assented to implied contracts. (Doc. 17 at 9 (quoting *Hummel v. Teijin Auto. Techs., Inc.*, No. 23-cv-10341, 2023 WL 6149059, at *11 (E.D. Mich. Sept. 20, 2023) ("Put succinctly, it is incredibly 'difficult to imagine, how, in our day and age of data and identity theft, the mandatory receipt of [PII] would not imply the recipient's assent to protect the information sufficiently.") (alteration in original)).) Defendant did not address this point in its reply.

In data-breach cases, a clear majority of courts, including several district courts within the Sixth Circuit, "have held that 'an implied contract is formed between an employer and employee when employees are required to provide personal information to their employer as a condition of their employment, and the resulting implied contract requires the employer to take reasonable steps to protect the employees' information.'" *In re Numotion*, 2025 WL 57712, at *8 (citing *Haney*, 2024 WL 4054361, at *11); *see also McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019) (holding that when the plaintiffs "as a condition of their employment [] had to provide personal information" to the defendant, the defendant "implicitly agreed to safeguard that information"). Many courts note that in this age of data and identity theft, the mandatory provision of PII to an employer implies the employer's assent to protect the information sufficiently. *Id.*; *see also Hummel*, 2023 WL 6149059, at *10 (noting that implied breach of contract claims in data-breach cases would be precluded if courts required hard proof of mutual assent because "it would be exceedingly difficult to show the recipient assented to those precise protective measures").

Here, Plaintiff alleges that he was required to provide his PII to Defendant as a condition of his employment. (Doc. 1-1 ¶ 68.) Plaintiff alleges Defendant "held itself out as a company dedicated to protecting the privacy" of PII (*id.* ¶ 113), and he and the class members conferred the benefit of their PII on Defendant "as a necessary part of receiving financial services" (*id.* ¶ 114).

Plaintiff argues that Defendant breached the implied contract when it failed to secure the PII, resulting in harm to Plaintiff and the class members. (*Id.* ¶¶ 116–17.) Viewing the facts in the light most favorable to Plaintiff, the Court finds Plaintiff adequately alleges the existence of an implied agreement, a meeting of the minds, and consideration to support the existence of an implied contract to engage in reasonable means to protect Plaintiff's PII. *See In re Numotion*, 2025 WL 57712, at *8. Therefore, Defendant's motion to dismiss Plaintiff's implied-contract claim will be **DENIED.**

4. Breach of Bailment

Lastly, the class-action complaint alleges a claim of breach of bailment. (Doc. 1-1 ¶¶ 118–122.) Under Tennessee law, "[a] bailment is a delivery of personalty for a particular purpose or on mere deposit, on a contract expressed or implied, that after the purpose has been fulfilled it shall be re-delivered to the person who delivered it or otherwise dealt with according to his direction or kept until he reclaims it." *Aegis Investigative Grp. v. Metro. Gov't of Nashville & Davidson Cty.*, 98 S.W.3d 159, 162–63 (Tenn. Ct. App. 2002). Bailees are merely temporary possessors, not owners of property. *Meade v. Paducah Nissan, LLC*, No. M2021-00563-COA-R3-CV, 2022 WL 2069160, at *4 (Tenn. Ct. App. June 9, 2022) (citing *Black's Law Dictionary* 162 (9th ed. 2009)).

While a bailment is usually created by contract, "an actual contract or one implied in fact is not always necessary." *Akers v. Prime Succession of Tenn., Inc.*, 387 S.W.3d 495, 510 (Tenn. 2012) (quoting *Aegis Investigative Grp*, 98 S.W.3d at 163) (internation quotations omitted). "In the absence of express contract, the creation of a bailment requires that possession and control pass from bailor to bailee; there must be full transfer, actual or constructive, so as to exclude the property from the possession of the owner and all other persons and give the bailee sole custody

and control for the time being." *Merritt v. Nationwide Warehouse Co.*, 605 S.W.2d 250, 253 (Tenn. Ct. App. 1980) (citation omitted).

Here, because there is no express contract, Plaintiff is required to show he gave Defendant sole custody and control of his PII. However, personal information is intangible and transfer of PII to one party does not limit transfer to another party. As Defendant notes, Plaintiff was free to use or disseminate his PII as he chose. (Doc. 20 at 8 (citing *McLaughlin v. Taylor Univ.*, 2024 WL 4274848, at *12 (N.D. Ind. Sept. 23, 2024) (noting that the case Plaintiff cites from the Northern District of Indiana is an outlier)).) Given the nature of PII, Plaintiff cannot allege he transferred exclusive possession of his PII to Defendant. *See Merritt*, 605 S.W.2d at 253; *see also In re Numotion*, 2025 WL 57712, at *12. Therefore, Plaintiff fails to state a claim for breach of bailment and Defendant's motion to dismiss Plaintiff's breach of bailment claim will be **GRANTED**. Plaintiff's breach of bailment claim will be **DISMISSED WITH PREJUDICE**.

IV. CONCLUSION

Accordingly, Defendant's motion to dismiss (Doc. 10) will be **GRANTED IN PART** and **DENIED IN PART**. The motion will be **GRANTED IN PART** as to Plaintiff's claims for negligence per se and breach of bailment. Plaintiff's claims for negligence per se and breach of bailment will be **DISMISSED WITH PREJUDICE**. The motion will be **DENIED IN PART** as to Plaintiff's claims for negligence and breach of implied contract.

In accordance with Rule 16(b) of the Federal Rules of Civil Procedure, a scheduling conference will be held on **April 17, 2025, at 3:30 p.m. Eastern.**

AN APPROPRIATE ORDER WILL ENTER.

/s/
CURTIS L. COLLIER
UNITED STATES DISTRICT JUDGE